UNITED STATES DISTRICT COURT

DISTRICT OF MAINE

UNITED STATES OF AMERICA	)	
	)	
	)	
	)	
v.	)	**CRIMINAL NO. 01-18-P-H**
	)	
FREDERICK W. BUTLER, JR.,	)	
	)	
DEFENDANT	)	

MEMORANDUM DECISION AND ORDER ON DEFENDANT'S MOTIONS TO SUPPRESS, DISMISS AND CONTINUE

The Indictment asserts that the defendant has previously been convicted of a crime relating to sexual abuse and abusive sexual conduct involving a minor or ward. It charges that four times thereafter, he knowingly and illegally received child pornography over the Internet, contrary to18 U.S.C. § 2252A(a)(2)((A). The defendant's motions to suppress, dismiss and continue are **DENIED**.

1. Students' Fourth Amendment Rights in University Computers

The Indictment charges that the images in question came over the Internet to computers at the Lewiston-Auburn College of the University of Maine. The defendant moves to suppress the University logs identifying when he used the University computers, as well as the contents of the hard drives from two University computers he used. I accept as true, for purposes of the motion, the assertions in the defendant's motion to suppress.

At the time, the defendant was a student enrolled in the University of Maine

system. Because he was an enrolled student, he had access to a computer lab on the Lewiston-Auburn campus. On one occasion, he left on a University computer screen a frozen image that a University employee considered pedophilia. That incident led to an investigation by University authorities, which revealed more such images on hard drives, and ultimately the police were involved. As a result, the prosecution now has the hard drives of two University computers, as well as session logs showing when the defendant used the computers. The defendant wants all of these suppressed as the product of searches in violation of the Fourth Amendment.

To assert a right under the Fourth Amendment, a defendant must demonstrate both a subjective expectation of privacy and an expectation that society judges as objectively reasonable. Kyllo v. United States, ___ U.S. ___, 2001 WL 636207, *3 (June 11, 2001); Rakas v. Illinois, 439 U.S. 128, 143 & n.12 (1978); Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). What that objectively reasonable expectation is for computers, under circumstances of shared usage, presents questions of some difficulty in today's environment of rapidly changing technology and provisions of service. I do not have to confront these difficult issues because the defendant has made not even a minimal showing that he had a reasonable expectation of privacy in either his session logs or the hard drives of these University-owned computers. Session logs are obviously maintained for the benefit of the University and therefore not suppressible on the defendant/student's motion. See Smith v.

Maryland, 442 U.S. 735, 742-44 (1979) (holding that a telephone customer had no legitimate expectation of privacy in telephone numbers he had dialed because in dialing he voluntarily conveyed the information to the telephone company and thereby assumed the risk that the telephone company would disclose it); United States v. Miller, 425 U.S. 435, 442 (1976) (holding that a bank depositor had no legitimate expectation of privacy in bank records that he voluntarily conveyed to the bank and that the bank used in the ordinary course of its business); United States v. Hambrick, 55 F. Supp.2d 504, 508-09 (W.D. Va 1999), aff'd, 25 F.3d 656 (4th Cir. 2000), cert. denied, ___ U.S. ___, 121 S.Ct. 832 (2001). As for the hard drives, the defendant has pointed to no computer privacy policies in effect at the University, no statements or representations made to him as a user of the computers in this lab, no practices concerning access to and retention of the contents of hard drives, not even password requirements. From all that appears, he, along with other students, was simply using the University computers under circumstances where images on the monitor were visible to others (as occurred here), and no commitments were made as to the privacy of hard drives. See United States v. Simons, 206 F.3d 392, 398-99 (4th Cir. 2000) (finding no reasonable expectation of privacy in files downloaded from the Internet to hard drives of employee's office computer where employer had express policy of monitoring Internet activities of employees).

The defendant relies upon "a legitimate and reasonable expectation of

privacy recognized by society in any work performed on, or documents and files produced on, computers he used while a student at the University of Maine." Pl.'s Mot. to Suppress at 3. Unlike the Supreme Court's treatment of generic payphone booths in 1967 in Katz, I conclude that in 2001 there is no generic expectation of privacy for shared usage on computers at large.[1] Conditions of computer use and access still vary tremendously. The burden remains on the defendant to show that his expectations were reasonable under the circumstances of the particular case. See United States v. Kimball, 25 F.3d 1, 9 (1st Cir. 1994). Without meeting that burden, he cannot challenge the University's decision to examine the computers he used, nor the warrant the police obtained later to search the hard drives of the University's computers.[2] (Even if he could challenge the warrant, he has also not satisfied the requirement for a Franks hearing for he has made no allegation of intentional or reckless falsehood. Franks v. Delaware, 438 U.S. 154, 155-56

[1] The commentators seem divided. Compare 1 Wayne R. LaFave Search & Seizure § 2.6 (3d. ed. Supp. 2001) (concluding that computer users do have a legitimate expectation of privacy in their electronic communications even when the system manager makes backup copies), and Randolph S. Sergent, Note, *A Fourth Amendment Model for Computer Networks and Data Privacy*, 81 Va. L. Rev. 1181, 1201-03 (1995) (same), with Note, *Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication*, 100 Harv. L. Rev. 1591, 1602 (1997) (stating that to be eligible for Fourth Amendment protection, a "cyberspace communicator" must "establish privacy vis-à-vis her system administrator and her communication must be hidden with some form of password, or possibly a gateway").

[2] I therefore do not address other interesting issues, some of which have been argued and some not: *e.g.*, Could the University as owner of the computers consent to the police search? See generally 3 Wayne R. LaFave Search & Seizure § 8.6 (3d ed. Supp. 2001); Sergent, 81 Va. L. Rev. at 1213-16. Were the actions of University employees themselves a search because as employees of a state institution they are state actors? Could the University employees nevertheless search without a warrant if the search was justified at its inception and reasonable in scope? See generally O'Connor v. Ortega, 480 U.S. 709, 723-26 (1987) (discussing government employer's search for work-related misconduct); New Jersey v. T.L.O., 469 U.S. 325, 337-42 (1985) (discussing school vice principal's search of student's purse).

(1978).)

2. Definition of Child Pornography

The First Circuit has already held that the definition of child pornography in 18 U.S.C. § 2256, applicable to 18 U.S.C. § 2252A, is not unconstitutionally overbroad or vague. United States v. Hilton, 167 F.3d 61, 71, 76 (1st Cir.), cert. denied, 528 U.S. 844 (1999). The fact that the United States Supreme Court has agreed to hear an apparently contrary decision from the Ninth Circuit, Free Speech Coalition v. Reno, 198 F.3d 1083, 1095-96 (9th Cir. 1999), cert. granted sub nom. Ashcroft v. Free Speech Coalition, ___ U.S. ___, 121 S. Ct. 876 (2001), does not change the applicable law in this Circuit or call for any continuance. If the Supreme Court should ultimately rule differently from the First Circuit, that ruling can then be grounds for appeal.

3. Commerce Powers

The provision of the federal statute under which the defendant is being prosecuted, 18 U.S.C. § 2252A(a)(2)(A), does not exceed Congress's commerce powers under the United States Constitution as the statute is applied in this case. The defendant is charged with knowingly receiving child pornography that had been transported in interstate and foreign commerce via the Internet to a computer at the Lewiston-Auburn College of the University of Maine. Thus, this prosecution involves direct regulation of the use of the channels of interstate commerce, one of Congress's traditional areas of authority. United States v.

Lopez, 514 U.S. 549, 558 (1995).[3]

SO ORDERED.

DATED THIS ____ DAY OF JUNE, 2001.

D. BROCK HORNBY
UNITED STATES DISTRICT JUDGE

[3] In other words, this prosecution does not involve a photograph handed over the backyard fence, or passed in a bedroom. If that were the subject of federal prosecution, with federal power being asserted only because the image in question at some previous time had moved in interstate commerce, there might well be some constitutional commerce clause issues in light of Lopez and United States v. Morrison, 529 U.S. 598 (2000). Compare United States v. Robinson, 137 F.3d 652, 655-56 (1st Cir. 1998) (upholding possession statute after Lopez but before Morrison), and United States v. Kallestad, 236 F.3d 225, 227-31 (5th Cir. 2000) (2-1 decision upholding possession statute after Lopez and Morrison), with United States v. Corp, 236 F.3d 325, 331-32 (6th Cir. 2001) (striking down possession statute as applied after Morrison).

U.S. District Court
District of Maine (Portland)
Criminal Docket For Case #: 01-CR-18-ALL

FREDERICK W BUTLER, JR.
defendant

BENET POLS, ESQ.
P.O. BOX 791
BRUNSWICK, ME 04011-0791
(207) 729-5154

U. S. ATTORNEYS:

GEORGE T. DILWORTH, AUSA
OFFICE OF THE U.S. ATTORNEY
P.O. BOX 9718
PORTLAND, ME 04104-5018
(207) 780-3257